In the Claims

Claim 1 (currently amended): A method of improving intrusion detection in a computing network, comprising steps of:

defining a plurality of intrusion suspicion levels for use when performing intrusion detection processing on inbound communications destined for a computing device on the computing network;

for each of a plurality of potential intrusion events, defining a set of at least one condition, wherein the set describes occurrence of ~~conditions which describe~~ the potential intrusion event;

associating one of the defined intrusion suspicion levels with each of the sets, wherein the associated intrusion suspicion level indicates how suspicious is an inbound communication matching each condition in the set ~~of conditions~~;

defining a plurality of sensitivity levels for filtering the inbound communications as potential intrusion events when performing the intrusion detection processing, each of the defined sensitivity levels usable for a different level of filtering of the inbound communications; and

performing the intrusion detection processing for a particular inbound communication received for the computing device, further comprising steps of:

determining whether each condition in any of the ~~at least one~~ sets ~~of conditions are~~ is matched for the particular inbound communication; and

if so, filtering the particular inbound communication by using a currently-applicable one of the defined sensitivity levels, in concert with the ~~dintrusion~~ intrusion suspicion level associated with the set for which each condition is [[the]] matched ~~conditions~~, to determine if the particular inbound communication should be treated as an intrusion event.

Claim 2 (canceled)

Claim 3 (currently amended): The method according to Claim 1, wherein the determining step further comprises comparing current conditions in the computing device to [[the]] corresponding conditions defined in at least one of the sets.

Claim 4 (previously presented): The method according to Claim 3, wherein the current conditions in the computing device comprise contents of the particular inbound communication.

Claim 5 (previously presented): The method according to Claim 4, wherein the current conditions in the computing device further comprise a protocol state of a protocol stack which processes the particular inbound communication.

Claim 6 (previously presented): The method according to Claim 1, further comprising the step of taking one or more defensive actions upon determining that the particular inbound communication should be treated as an intrusion event.

Claim 7 (original): The method according to Claim 6, wherein the defensive actions are determined by consulting intrusion detection policy information.

Claim 8 (previously presented): The method according to Claim 7, wherein the intrusion

detection policy information is stored in a network-accessible repository.

Claim 9 (currently amended): The method according to Claim 1, wherein ~~the defined~~ at least one of the defined sets ~~set of conditions~~ represents ~~one or more~~ an attack ~~signatures~~ signature.

Claim 10 (currently amended): The method according to Claim [[9]] 1, wherein at least one of the defined sets represents ~~attack signatures is~~ a class signature ~~representing~~ for a class of attacks.

Claim 11 (currently amended): The method according to Claim 1, wherein each of the ~~at least one set of conditions is specified as as~~ defined sets comprises a condition part in an intrusion detection rule, and wherein each of the intrusion detection rules further specifies at least one action to be taken upon determining that the particular inbound communication should be treated as an intrusion event.

Claim 12 (previously presented): The method according to Claim 1, wherein the performing step operates in the computing device for which the particular inbound communication is destined.

Claim 13 (previously presented): The method according to Claim 12, wherein the performing step operates within layer-specific intrusion detection logic executing in a protocol stack running on the computing device.

Claim 14 (previously presented): The method according to Claim 1, wherein the performing step

operates in a network device which analyzes communications directed to the computing device for which the particular inbound communication is destined.

Claim 15 (currently amended): The method according to Claim 1, wherein the [[using]] filtering step further comprises ~~consulting~~ using the currently-applicable one of the defined sensitivity levels and the intrusion suspicion level associated with the matched set to consult a stored mapping that indicates, for ~~between~~ each combination of one of the defined sensitivity levels and [[each]] one of the defined intrusion suspicion levels, whether an inbound communication corresponding to that combination ~~using the currently-applicable one of the defined sensitivity levels and the intrusion suspicion level associated with the matched conditions, to determine if the particular inbound communication~~ should be treated as an intrusion event.

Claims 16 - 21 (canceled)

Claim 22 (currently amended): A system for improving intrusion detection in a computing network, comprising:

a definition of a plurality of intrusion suspicion levels ~~defined~~ for use when performing intrusion detection processing on inbound communications destined for a computing device on the computing network;

for each of a plurality of potential intrusion events, a ~~defined~~ definition of a set of at least one condition, wherein the set describes occurrence of ~~conditions which describe~~ the potential intrusion event;

means for associating one of the defined intrusion suspicion levels with each of the defined sets, wherein the associated intrusion suspicion level indicates how suspicious is an inbound communication matching each condition in the set ~~of conditions~~;

a definition of a plurality of sensitivity levels ~~defined~~ for filtering the inbound communications as potential intrusion events when performing the intrusion detection processing, each of the defined sensitivity levels usable for a different level of filtering of the inbound communications; and

means for performing the intrusion detection processing for a particular inbound communication received for the computing device, further comprising:

means for determining whether each condition in any of the ~~at least one defined~~ sets ~~of conditions are~~ is matched for the particular inbound communication; and

if so, means for filtering the particular inbound communication by using a currently-applicable one of the defined sensitivity levels, in concert with the intrusion suspicion level associated with the set for which each condition is matched ~~conditions~~, to determine if the particular inbound communication destined for the computing device should be treated as an intrusion event.

Claim 23 (canceled)

Claim 24 (currently amended): The system according to Claim 22, wherein the means for determining further comprises means for comparing current conditions in the computing device to [[the]] corresponding conditions defined in at least one of the sets.

Claim 25 (previously presented): The system according to Claim 22, further comprising means for taking one or more defensive actions upon determining that the particular inbound communication should be treated as an intrusion event, wherein the defensive actions are determined by consulting intrusion detection policy information.

Claim 26 (currently amended): The system according to Claim 22, wherein each of the ~~at least one set of conditions is specified as~~ defined sets comprises a condition part in an intrusion detection rule, and wherein each of the intrusion detection rules further specifies at least one action to be taken upon determining that the particular inbound communication should be treated as an intrusion event.

Claim 27 (currently amended): The system according to Claim 22, wherein the means for [[using]] filtering further comprises means for using the currently-applicable one of the defined sensitivity levels and the intrusion suspicion level associated with the matched set to consult ~~consulting~~ a stored mapping that indicates, for ~~between~~ each combination of one of the defined sensitivity levels and [[each]] one of the defined intrusion suspicion levels, whether an inbound communication corresponding to that combination ~~using the currently-applicable one of the defined sensitivity levels and the intrusion suspicion level associated with the matched conditions, to determine if the particular inbound communication~~ should be treated as an intrusion event.

Claims 28 - 31 (canceled)

Claim 32 (currently amended): A computer program product for improving intrusion detection in a computing network, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code defining a plurality of intrusion suspicion levels for use when performing intrusion detection processing on inbound communications destined for a computing device on the computing network;

for each of a plurality of potential intrusion events, computer-readable program code defining a set of at least one condition, wherein the set describes occurrence of ~~conditions which describe~~ the potential intrusion event;

computer-readable program code associating one of the defined intrusion suspicion levels with each of the sets, wherein the associated intrusion suspicion level indicates how suspicious is an inbound communication matching each condition in the set ~~of conditions~~;

computer-readable program code defining a plurality of sensitivity levels for filtering the inbound communications as potential intrusion events when performing the intrusion detection processing, each of the defined sensitivity levels usable for a different level of filtering of the inbound communications; and

computer-readable program code for performing the intrusion detection processing for a particular inbound communication received for the computing device, further comprising:

computer-readable program code for determining whether each condition in any of the ~~at least one~~ sets ~~of conditions are~~ is matched for the particular inbound communication; and

if so, computer-readable program code for filtering the particular inbound

communication by using a currently-applicable one of the defined sensitivity levels, in concert with the intrusion suspicion level associated with the matched ~~conditions~~ set, to determine if the particular inbound communication should be treated as an intrusion event.

Claim 33 (canceled)

Claim 34 (currently amended): The computer program product according to Claim 32, wherein the computer-readable program code for determining further comprises computer-readable program code for comparing current conditions in the computing device to [[the]] corresponding conditions defined in at least one of the sets, the current conditions in the computing device comprising contents of the particular inbound communication.

Claim 35 (currently amended): The computer program product according to Claim 32, wherein the computer-readable program code for determining further comprises computer-readable program code for comparing current conditions in the computing device to [[the]] corresponding conditions defined in at least one of the sets, the current conditions in the computing device comprising contents of the particular inbound communication and a protocol state of a protocol stack which processes the particular inbound communication.

Claim 36 (previously presented): The computer program product according to Claim 32, further comprising computer-readable program code for taking one or more defensive actions upon determining that the particular inbound communication should be treated as an intrusion event,

wherein the defensive actions are determined by consulting intrusion detection policy information stored in a policy repository.

Claim 37 (currently amended): The computer program product according to Claim 32, wherein ~~the defined~~ at least one of the defined sets ~~set of conditions~~ represents ~~one or more~~ an attack ~~signatures~~ signature, and wherein at least one of the attack signatures is a class signature representing a class of attacks.

Claim 38 (previously presented): The computer program product according to Claim 32, wherein the computer-readable program code for performing operates in the computing device for which the particular inbound communication is destined.

Claim 39 (previously presented): The computer program product according to Claim 32, wherein the computer-readable program code for performing operates in a network device which analyzes communications directed to the computing device for which the particular inbound communication is destined.

Claim 40 (currently amended): The computer program product according to Claim 32, wherein the computer-readable program code for [[using]] filtering further comprises computer-readable code for ~~consulting~~ using the currently-applicable one of the defined sensitivity levels and the intrusion suspicion level associated with the matched set to consult a stored mapping that indicates, for ~~between~~ each combination of one of the defined sensitivity levels and [[each]] one of

the defined intrusion suspicion levels, whether an inbound communication corresponding to that combination ~~using the currently-applicable one of the defined sensitivity levels and the intrusion suspicion level associated with the matched conditions~~ set, ~~to determine if the particular inbound communication~~ should be treated as an intrusion event.

Claims 41 - 44 (canceled)

Claim 45 (currently amended): The method according to Claim 6, wherein the defensive actions are specified as actions in a rule in which the matched ~~conditions are~~ set is specified.

Claim 46 (previously presented): The method according to Claim 6, wherein at least one of the defensive actions comprises discarding the particular inbound communication.

Claim 47 (previously presented): The method according to Claim 6, wherein at least one of the defensive actions comprises limiting at least one of resources or traffic associated with a connection on which the particular inbound communication is received.

Claim 48 (previously presented): The method according to Claim 6, wherein at least one of the defensive actions comprises dynamically dropping a deny filter into the computing network to shun subsequent traffic.

Claim 49 (previously presented): The method according to Claim 6, wherein at least one of the

defensive actions comprises reporting the intrusion event to one or more entities.

Claim 50 (previously presented): The method according to Claim 49, wherein reporting the intrusion event to one or more entities further comprises sending an alert to a management component external from the computing device for which the particular inbound communication is destined.

Claim 51 (previously presented): The method according to Claim 49, wherein reporting the intrusion event to one or more entities further comprises writing at least one event record to at least one of a system log and a console.

Claim 52 (previously presented): The method according to Claim 49, wherein reporting the intrusion event to one or more entities further comprises recording inbound communications associated with the intrusion event in at least one of a trace or other repository.

Claim 53 (previously presented): The method according to Claim 49, wherein reporting the intrusion event to one or more entities further comprises writing statistics records on normal behavior to establish baselines as to what constitutes abnormal behavior for the inbound communications.

Claim 54 (currently amended): The method according to Claim 1, wherein at least one of the defined sets ~~of conditions~~ specifies a current system state of the computing device.

Claim 55 (currently amended): The method according to Claim 1, wherein at least one of the defined sets ~~of conditions~~ specifies at least one threshold reached at the computing device.

Claim 56 (currently amended): The method according to Claim 1, wherein at least one of the defined sets ~~of conditions~~ specifies at least one state transition to be caused, at the computing device, upon receiving the particular inbound communication.

Claim 57 (previously presented): The method according to Claim 1, wherein the currently-applicable sensitivity level is specified, for the computing device, by a systems administrator.

Claim 58 (previously presented): The method according to Claim 1, wherein the currently-applicable sensitivity level is specified, for the computing device, by configuration data in a stored repository.